**Publishing Remote Desktop Services With Web Application Gateway**

[**Home**](https://www.petenetlive.com/)»[**Active Directory**](https://www.petenetlive.com/KB/Article/category/microsoft/active-directory)»Publishing Remote Desktop Services With Web Application Gateway

[Publishing Remote Desktop Services With Web Application Gateway | PeteNetLive](https://www.petenetlive.com/KB/Article/0001143)

***https://www.petenetlive.com/KB/Article/0001143KB ID*** 0001143

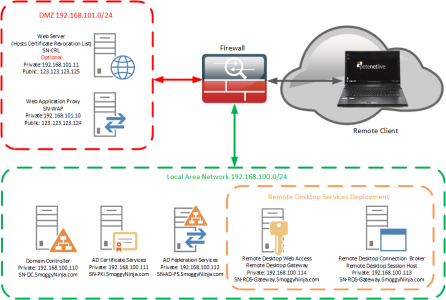
Problem

Getting this article to completion has been a bit of a journey! This is the final post that will stitch together all the others I’ve posted over the last couple of weeks, that will enable you to publish your RemoteApps with  ‘Remote Desktop Web Access’, and have that service presented securely from your DMZ. I’ll be using Active Directory Federation Services, (you don’t have to, but it’s more secure than simply using ‘pass-though’ security).

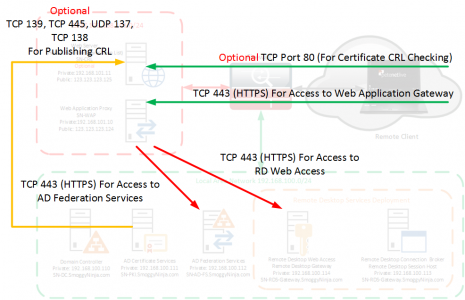
Solution

**Prerequisites**

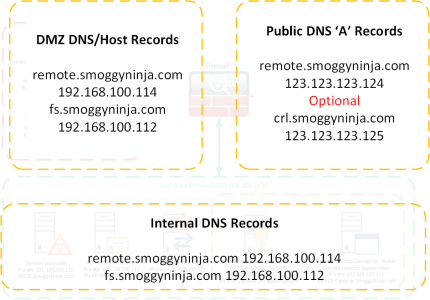
**Topology**: Simply getting your ‘ducks in a row’ will take a lot longer than actually deploying the service. Here is the topology that I’m going to deploy;

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00040-1.png)

**Firewall Rules**: You will see I’ve labelled all the Certificate/CRL rules as optional, this is because you would only need them if you were using self signed certificates. In this example that’s what I am doing, this means that all my remote clients need the root certificate installing on them, so for production I suggest you purchase a publicly signed wildcard certificate for simplicity.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00042.png)

**DNS Requirements**: For your internal domain and the DMZ it’s simple enough but your external clients will need to be able to resolve your public URL (and the URL of your CRL is used).

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00044.png)

**Certificate Services** (Optional): If you want to deploy self signed wildcard certificates you will  need a PKI environment and a published CRL. See the following article;

[**Windows Certificate Services – Setting up a CRL**](http://www.petenetlive.com/KB/Article/0000957)

Once setup you will need to generate a self signed wildcard certificate. See the following article;

[**Certificate Services – Create a ‘Wildcard Certificate’**](http://www.petenetlive.com/KB/Article/0001128)

**Active Directory Directory Services:** You need to have your ADFS farm deployed and ready to add your relying trust to. See the following article;

[**Deploy Active Directory Federation Services**](http://www.petenetlive.com/KB/Article/0001140)

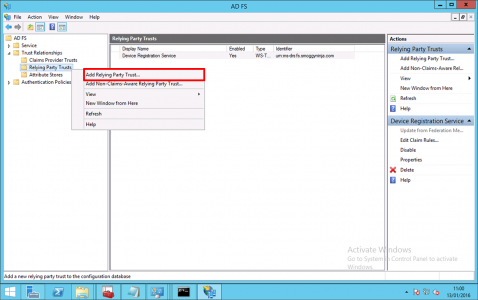
**Web Application Proxy**: The Role needs installing ready to have the publishing rule added for Remote Desktop Web Access. See the following article;

[**Deploying Windows ‘Web Application Proxy’**](http://www.petenetlive.com/KB/Article/0001142)

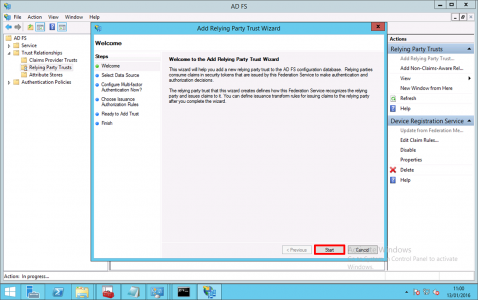
MAKE SURE: You have ran Windows updates on the WAP server, there are a number of bugs that have been fixed, ensure you have at least [**KB2975719**](https://support.microsoft.com/en-us/kb/2975719), and in addition you need to have [**KB2983037 Hotfix**](https://support.microsoft.com/en-us/kb/2982037) installed.

Step 1: Add A Relying Trust To Active Directory Federation Services For Web Application Proxy

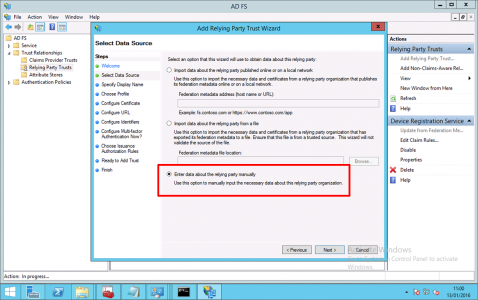
On your ADFS Server > Administrative Tools > AD FS Management > AD FS > Trust Relationships > Relying Party Trusts > Add Relying Party Trust.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00001-20.png)

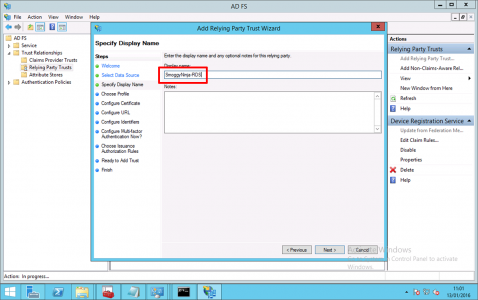
Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00002-15.png)

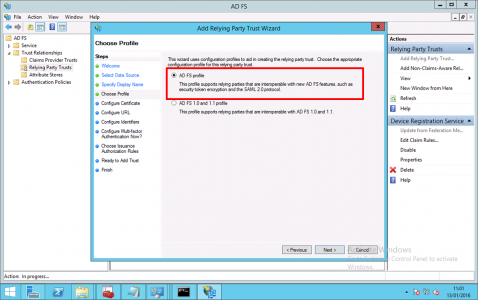
Enter data about relying party trust manually > Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00003-10.png)

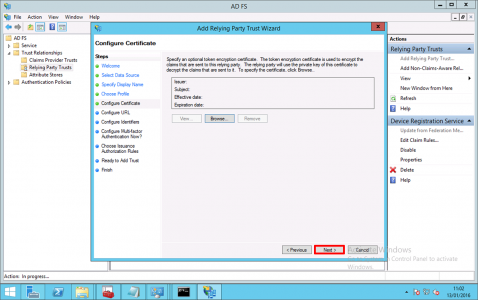
Give the trust a name > Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00004-8.png)

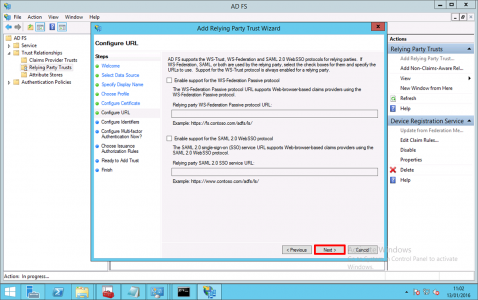
AD FS Profile  > Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00005-7.png)

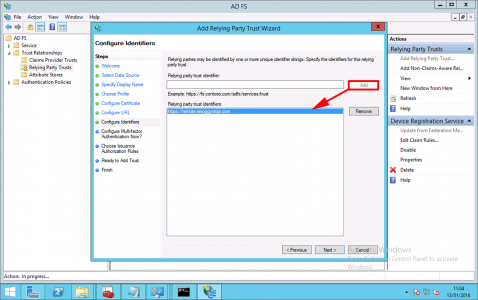
Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00006-7.png)

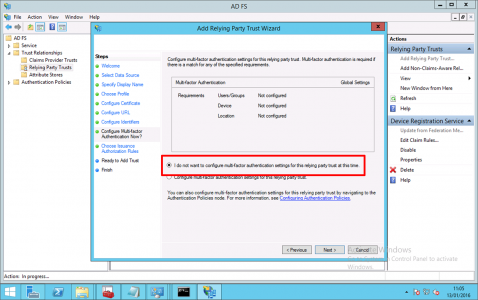
Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00007-6.png)

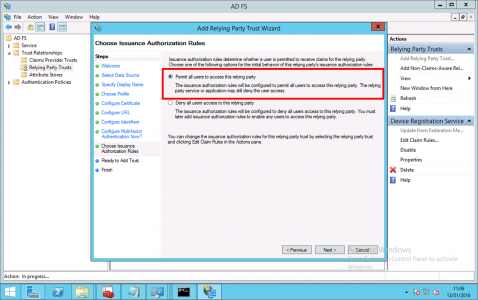
As an identifier, add in the UEL to access Remote Desktop Web Access > Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00008-5.png)

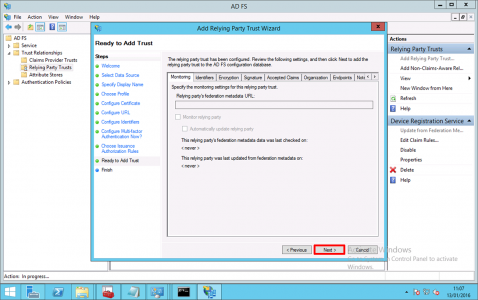
I do not want to configure multi-factor authentication settings for this relying  party trust at this time > Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00009-5.png)

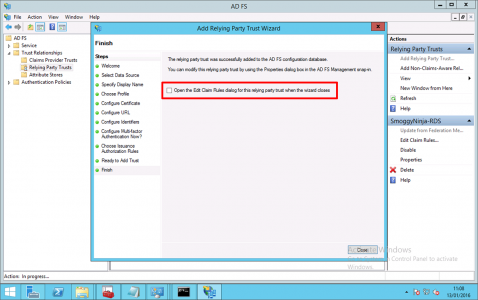
Permit all users to use this relying party > Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00010-5.png)

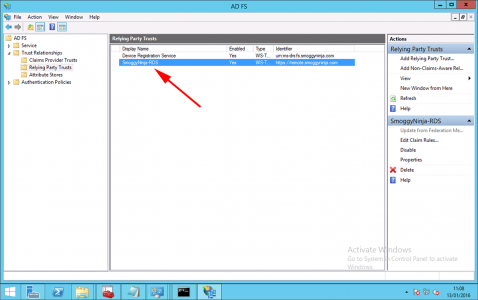
Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00011-3.png)

Untick “Open Edit Claim Rules dialog  for this relying party trust when the wizard closes’ > Close.

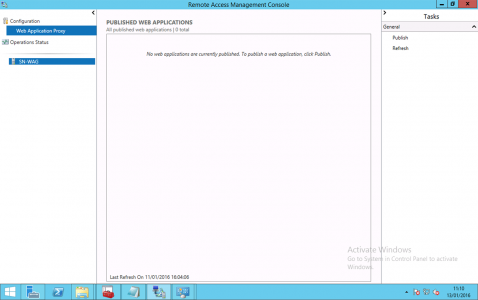
[](http://www.petenetlive.com/wp-content/uploads/2016/01/00012-3.png)

You should see your relying part trust listed, take note of its name.

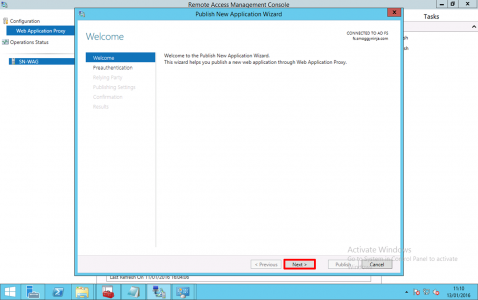
[](http://www.petenetlive.com/wp-content/uploads/2016/01/00013-3.png)

Step 2: Configure Web Application Proxy To Publish Remote Desktop Web Access

On the WAP Server > Administrative Tools > Remote Access Management > Select the Server > Publish.

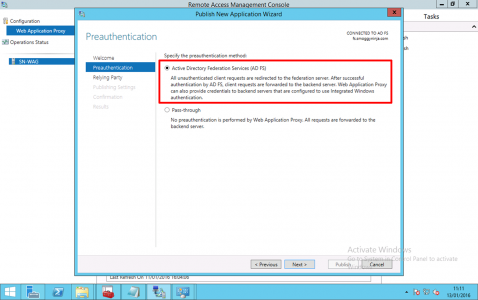
[](http://www.petenetlive.com/wp-content/uploads/2016/01/00020-2.png)

Next.

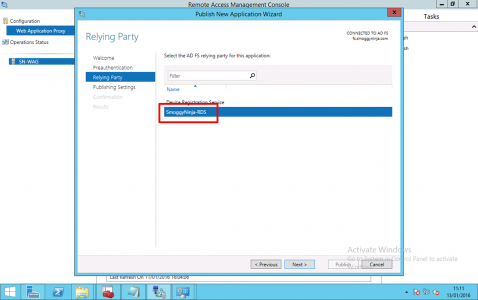
[](http://www.petenetlive.com/wp-content/uploads/2016/01/00021-2.png)

Select ‘Active Directory Federation Services (AD FS) > Next.

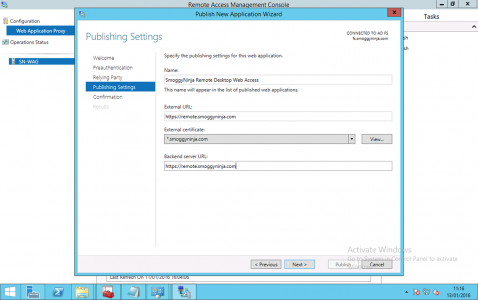
**Note**: As mentioned above, you can choose ‘pass-through’, then author authentication is done on the internal RD Web Access server (which is less secure).

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00022-2.png)

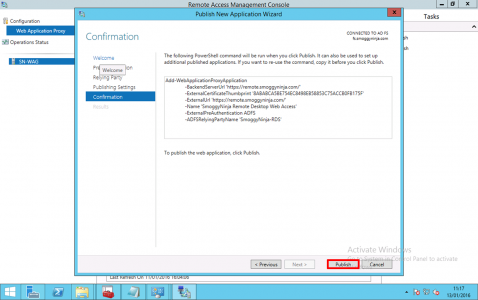
Select the relying trust you created above > Next. (If it’s not there check https is open, and you can resolve the AD FS service name) > Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00023-2.png)

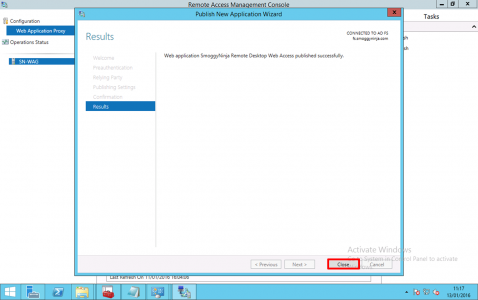
Give the publishing rule a name, and enter the URL the service will be published on, (this is usually the same inside and outside but does not have to be) >  Select your wildcard certificate > Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00024-2.png)

Publish.

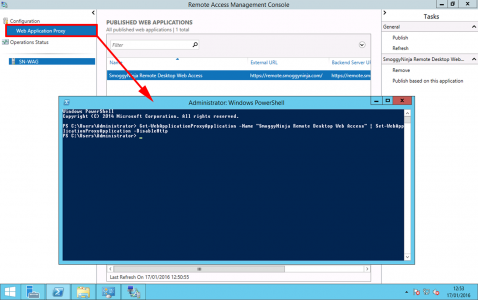
[](http://www.petenetlive.com/wp-content/uploads/2016/01/00025-2.png)

Close

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00026-2.png)

In PowerShell execute the following command;

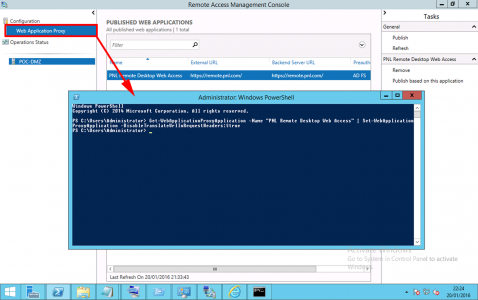
Get-WebApplicationProxyApplication -Name “SmoggyNinja Remote Desktop Web Access” | Set-WebApplicationProxyApplication -DisableHttp

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00027-2.png)

Then the following command;

Get-WebApplicationProxyApplication -Name “SmoggyNinja Remote Desktop Web Access” | Set-WebApplicationProxyApplication -DisableTranslateUrlInRequestHeaders:$true

**Note**: You only actually need this command if you’re  using different URLs but let’s stick with a script that works.

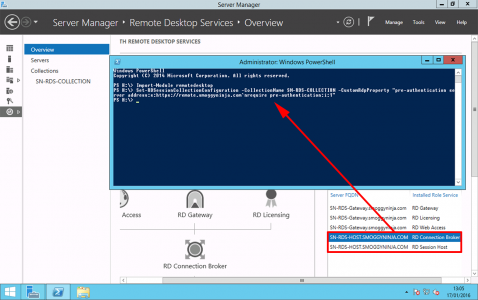
[](http://www.petenetlive.com/wp-content/uploads/2016/01/00029-2.png)

Step 3: Additional Works.

On the Remote Desktop Session Host Server run the following commands;

Import-Module Remote Desktop

Set-RDSessionCollectionConfiguration -CollectionName SN-RDS-COLLECTION -CustomRdpProperty “pre-authentication server address:s:https://remote.smoggyninja.com`nrequire pre-authentication:i:1″

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00028-2.png)

Related Articles, References, Credits, or External Links

NA

Tom Murphy's Blog

Securing RD Gateway with Web Application Proxy - Part 2

### Picking up where we left off...

Welcome to Part 2 of my series "Securing RD Gateway with Web Application Proxy." In [Part 1 of the series](https://web.archive.org/web/20180619155432/http:/frozentundrait.blogspot.com/2015/05/securing-rd-gateway-with-web.html), we had left off after installing AD Federation Services and Web Application Proxy. In addition to the installation, we also performed basic configuration of both products. In Part 2 of the series, we'll start configuring the pieces needed specifically to get RD Web Access and RD Gateway working behind Web Application Proxy.

### Creating the Relying Party Trust in ADFS

Now that ADFS and WAP are both installed, the next step is to create a trust relationship between ADFS and RDS. This is accomplished by creating a **Relying Party Trust** within the ADFS Management console. Switch to the ADFS server, and from Server Manager, click Tools and select AD FS Management. In the ADFS Management console, expand **Trust Relationships**, right-click on **Relying Party Trusts**, and select **Add Relying Party Trust** from the context menu.  
 **\*\*\*NOTE\*\*\*** - I originally tried adding a Non-Claims-Aware trust, but this was unsuccessful. After speaking with an engineer from Microsoft, he explained that RDS actually isn't fully claims-aware, but to create a claims-aware trust anyways to get everything working behind Web Application Proxy.

|  |
| --- |
|  |
| Adding the Relying Party Trust |

The **Add Relying Party Trust Wizard** will open. Click the **Start** button to begin.

|  |
| --- |
|  |
| Adding the Relying Party Trust |

Select the bottom option to **Enter data about the relying party manually** and click **Next**.

|  |
| --- |
|  |
| Adding the Relying Party Trust |

Enter a **name** and **description** for the trust, and click **Next**.

|  |
| --- |
|  |
| Adding the Relying Party Trust |

Leave the default of **AD FS profile** and click **Next**.

|  |
| --- |
|  |
| Adding the Relying Party Trust |

Optionally select a token encryption certificate. We'll be skipping this step for this demo. Click **Next**.

|  |
| --- |
|  |
| Adding the Relying Party Trust |

Leave the default options, as we'll be relying on the WS-Trust protocol. Click **Next**.

|  |
| --- |
|  |
| Adding the Relying Party Trust |

For the Relying party trust identifier, enter the **external URL** that is used to access your RD Web Access and RD Gateway. Only enter the base URL, do not add \RDWeb or any sub-directories. Click the **Add** button to add the identifier, and then click **Next**.

|  |
| --- |
|  |
| Adding the Relying Party Trust |

ADFS Multi-factor Authentication is outside the scope of this post, so leave the default option of **I do not want to configure multi-factor authentication settings for this relying party trust at this time** and click **Next**.

|  |
| --- |
|  |
| Adding the Relying Party Trust |

Select the default option of **Permit all users to access this relying party** and click **Next**.

|  |
| --- |
|  |
| Adding the Relying Party Trust |

Click **Next** to add the trust.

|  |
| --- |
|  |
| Adding the Relying Party Trust |

Uncheck the box to edit claim rules, and click the **Close** button to complete the wizard.

|  |
| --- |
|  |
| Finished with the Relying Party Trust |

Back in the ADFS Management console, you should now see your RDS relying party trust listed.

|  |
| --- |
|  |
| The newly added Relying Party Trust for RDS |

### Publishing RD Gateway behind Web Application Proxy

OK, so let's recap quickly. We've installed ADFS and configured it with our certificate. We've installed WAP and pointed it at the ADFS server. We've created the Relying Party Trust in ADFS for RDS. The next step is to publish RD Gateway through WAP.  
  
Connect to your WAP server and switch to the Remote Access Managament console. In the left pane, make sure Web Application Proxy is selected, and then in the right pane, click **Publish**.

|  |
| --- |
|  |
| Publishing RD Gateway |

The **Publish New Application Wizard** will open. Click **Next**.

|  |
| --- |
|  |
| Publishing RD Gateway |

For the preauthentication, select **Active Directory Federation Services (AD FS)** and click **Next**.

|  |
| --- |
|  |
| Publishing RD Gateway |

Select the Relying Party Trust that we created earlier, and click **Next**.

|  |
| --- |
|  |
| Publishing RD Gateway |

Choose a name for this published application - this is for internal use only. Enter the external URL that users will use to access your RD Gateway/RD Web Access installations, and then select the certificate used by your RD Gateway. Make sure the backend server URL is the same as the external URL. Click **Next**.

|  |
| --- |
|  |
| Publishing RD Gateway |

Click **Publish**.

|  |
| --- |
|  |
| Publishing RD Gateway |

Finally, click **Close** to finish the wizard.

|  |
| --- |
|  |
| Publishing RD Gateway... complete! |

You should now see your published web application in the Remote Access Management console.

|  |
| --- |
|  |
| Our brand-new published web app |

Next, we need to customize a few of the settings for the published web proxy, which can only be done with PowerShell. We need to modify two settings:

* DisableHttpOnlyCookieProtection - this is required for RD Gateway to function correctly.
* InactiveTransactionsTimeoutSec - how often an idle session will reset. The default is 300 seconds, meaning if a user's RemoteApp goes idle, it will reset the connection every five minutes - not something we want to happen.

Open a PowerShell window with elevated credentials (run as administrator) and enter the following command:

[?](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html)

|  |  |
| --- | --- |
| 1 | Get**-WebApplicationProxyApplication** **-Name** "AppName\_Here" | **Set-WebApplicationProxyApplication** **-DisableHttpOnlyCookieProtection**:$true **-InactiveTransactionsTimeoutSec** 28800 |

**\*\*\*NOTE\*\*\*** - This command won't work if you didn't install [KB2982037 (HttpOnly Update)](https://web.archive.org/web/20180619155432/https:/support.microsoft.com/en-us/kb/2982037) per the prerequisites - do so now if you haven't already.

|  |
| --- |
|  |
| Modifying the DisableHttpOnlyCookieProtection and InactiveTransactionsTimeoutSec properties |

The last step in publishing a web application through WAP is to ensure the server can forward correctly to the internal URL of the web application. If your internal DNS name resolution is working fine, then you are good, but otherwise the easiest way to ensure the WAP server forwards correctly is to modify the HOSTS file on your WAP server.  
  
Create an entry in the HOSTS file pointing the internal URL to the correct IP address of your RD Gateway server.

|  |
| --- |
|  |
| Modifying the HOSTS file on the WAP server |

### Modifying your RDS Collections

At this point, you should be able to access the external URL for your RDS environment, be prompted by the ADFS pre-authentication page, successfully login and get passed onto RD Web Access. However if you try to access a published RemoteApp - it will fail to connect!  
  
We need to modify both the session collections and virtual desktop collections with a custom RDP property so that the RD Gateway knows how to retrieve the ADFS edge token from the browser, in order to get past WAP.  
  
Connect to your RD Connection Broker server, open a PowerShell window and type the following commands:

[?](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html)

|  |  |
| --- | --- |
| 1  2 | Import**-Module** remotedesktop  **Set-RDSessionCollectionConfiguration** **-CollectionName** <collection\_name\_here> **-CustomRdpProperty** "pre-authentication server address:s:[https://<external\_URL\_here](https://web.archive.org/web/20180619155432mp_/https:/%3Cexternal_URL_here)>`nrequire pre-authentication:i:1" |
|  |
| Modifying a test collection with the pre-authentication settings |

Notice for the pre-authentication server address property, the URL is the same as the published URL in WAP. You do not need to add /RDWeb at the end of the URL.  
  
You'll need to enter this command for each RDS session collection in your environment. Here's the equivalent command for a virtual desktop collection:

[?](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html)

|  |  |
| --- | --- |
| 1  2 | Import**-Module** remotedesktop  **Set-RDVirtualDesktopCollectionConfiguration** **-CollectionName** <collection\_name\_here> **-CustomRdpProperty** "pre-authentication server address:s:[https://<external\_URL\_here](https://web.archive.org/web/20180619155432mp_/https:/%3Cexternal_URL_here)>/rdweb `nrequire pre-authentication:i:1" |

Once you've set the pre-authentication settings on each session collection and virtual desktop collection, you'll be able to successfully launch RemoteApps and connect to VDI collections via RD Web Access.

### Modifying Desktops.aspx

In addition to modifying each Session Collection and Virtual Desktop Collection, if you utilize RD Web Access and the "**Connect to a remote PC**" link to allow users to remotely access their work computers, you'll also need to modify the **Desktops.aspx** page to add the pre-authentication RDP properties.  
  
Navigate to **C:\Windows\Web\RDWeb\Pages\en-US** and open **Desktops.aspx** in the text editor of your choice, and search for the following string:

[?](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html)

|  |  |
| --- | --- |
| 1 | RDPstr += "getUserNameRdpProperty(); |

Just **BEFORE** that line of code, add the following two lines of text:

[?](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html)

|  |  |
| --- | --- |
| 1  2 | RDPstr += "pre-authentication server address:s:[https://<external\_URL\_here](https://web.archive.org/web/20180619155432mp_/https:/%3Cexternal_URL_here)>\n";  RDPstr += "require pre-authentication:i:1\n"; |
|  |
| Modifying Desktops.aspx with preauthentication settings |

Just like when modifying your Session Collections, enter the URL without adding /RDWeb at the end.  
  
Save the file. Now when you remote into a machine via RD Web Access, you'll be able to connect successfully.

### Conclusion

That's about it. If you've followed the instructions, you should have RD Web Access and RD Gateway working behind Web Application Proxy, with AD Federation Services for preauthentication.

Posted by [Tom Murphy](https://web.archive.org/web/20180619155432/https:/plus.google.com/103453455369744944883)at [10:16 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html)

[Email This](https://web.archive.org/web/20180619155432/https:/www.blogger.com/share-post.g?blogID=2693747771068034275&postID=7482951584067192238&target=email)[BlogThis!](https://web.archive.org/web/20180619155432/https:/www.blogger.com/share-post.g?blogID=2693747771068034275&postID=7482951584067192238&target=blog)[Share to Twitter](https://web.archive.org/web/20180619155432/https:/www.blogger.com/share-post.g?blogID=2693747771068034275&postID=7482951584067192238&target=twitter)[Share to Facebook](https://web.archive.org/web/20180619155432/https:/www.blogger.com/share-post.g?blogID=2693747771068034275&postID=7482951584067192238&target=facebook)[Share to Pinterest](https://web.archive.org/web/20180619155432/https:/www.blogger.com/share-post.g?blogID=2693747771068034275&postID=7482951584067192238&target=pinterest)

Labels: [ADFS](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/search/label/ADFS), [RDS](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/search/label/RDS), [Web Application Proxy](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/search/label/Web%20Application%20Proxy)

#### 52 comments:

1. 

[**Adam McIntosh**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/10989831025135979939)[June 17, 2015 at 6:35 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1434584113654#c4219976228158203688)

Tom, does this allow you to use a RDP file externally with the RDP geatway settings saved in it? or do you have to login to RDweb and then use the Connect to a remote PC feature?

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17674111757513001655)[June 17, 2015 at 9:39 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1434595141498#c8643837815462692163)

Hi Adam, following this guide will explicitly PREVENT using a saved RDP file. The reason is because of using the ADFS preauthentication. Basically WAP won't pass the connection to the backend server unless you have authenticated against ADFS first. When you authenticate, WAP issues a cookie to your browser (also called an edge token) that allows the traffic to flow past WAP and onto the backend server. When using a saved RDP file, you won't have access to the edge token, and WAP will block the traffic.  
  
That being said, the real use case for setting up RD Gateway behind WAP in this manner is if you want to force your users to login using RDWeb. In my case, we have a third party two-factor authentication product that integrates with the RDWeb login page. Users were saving RDP files and using mstsc.exe to skip RDWeb and connect directly to RD Gateway, essentially bypassing our 2FA. By setting up WAP with ADFS preauthentication, we are preventing this backdoor access and forcing users to user RDWeb and 2FA.

* 1. 

[**Adam McIntosh**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/10989831025135979939)[June 18, 2015 at 5:14 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1434665658167#c5672967979066806407)

Thanks for the response, I am trying to design a solution for external contractors to get in to our network and have put this option on the table.  
Thanks

[**Reply**](javascript:;)

1. 

[**Joshua Goss**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/15782624733807085351)[June 18, 2015 at 12:51 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1434649912597#c4451430371766280263)

Hi Tom, great post, thanks. Couple of questions. Where does your RDS Gateway/Web server sit in your network, the DMZ or WAN? What if any ports did you have to open to it from the WAN or does it flow through the Web proxy? Also, any recommendations on 2FA solution?

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17674111757513001655)[June 18, 2015 at 11:00 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1434686455316#c7888528993679264898)

Hi Joshua, you'll want the WAP server in the DMZ network, as that is what users will be directly connecting through. ADFS and RD Gateway/RD Web Access can actually be in your internal network. You'll only need ports 80/443 open on the external firewall to the WAP server. The internal firewall is a little trickier, you'll need 80/443 open between the WAP server and the RD Gateway/RD Web Access server, but you'll also need to open 443 between the WAP and ADFS servers. In my testing, I could only get this working properly if the WAP server was a member of the internal domain, so you'll need to open standard ports for AD/DNS/Kerberos, etc.

[**Reply**](javascript:;)

1. 

[**DanB**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/06018010748225789882)[June 26, 2015 at 7:34 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1435322046194#c1278890445939219543)

Hi Tom,  
  
Thank you for the great post, does this auto sign you in to the RDWEB page and also are you prompted for credentials when launching a RemoteApp?

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17674111757513001655)[June 26, 2015 at 10:40 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1435376439654#c2311679112589885789)

Hi Dan,  
  
Unfortunately the user will NOT automatically be signed into the RDWeb page - that sort of integration between WAP and RDWeb just isn't there yet - though when I spoke with Microsoft, they did make mention of that functionality possibly being included with the next version of WAP in Windows Server 2016.  
  
The good news, however, is that RDWeb SSO continues to function when launching RemoteApps as expected. So as long as you have the proper certificates and SSO is working before WAP, it will continue to function after WAP.

[**Reply**](javascript:;)

1. 

[**shubh**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/13006509687646399309)[June 30, 2015 at 8:33 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1435671196639#c551762156285278524)

Hi Tom,  
  
Thanks for your excellent article.  
  
However, prior to seeing this article, i had published RDWeb (& Gateway) using Non-Claim aware application template. I was able to access RDWeb and SSO was also working fine. While launching any remote applicaition, i was being prompted for credentials and even though i was providing correct credentials, i was not able to login.  
  
Now, after reading this article, i have changed that to claim aware application. Although, i am able to login and launch application but i am being prompted for credentials three time. First is form based authentication from WAP/ADFS, second from RDWeb and then third one from while launching the Remote App.  
  
Can you please suggest if it is possible to achieve SSO?  
  
Regards  
Shubham

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17674111757513001655)[June 30, 2015 at 6:47 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1435708049593#c1955432413106828)

Hi Shubham,  
  
Does SSO work when accessing RDWeb/RD Gateway directly, without WAP/ADFS in the picture? Typically if SSO is not working, it's a problem with your certificates. I would suggest looking down that route.

* 1. 

[**shubh**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/13006509687646399309)[July 8, 2015 at 6:30 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1436355038086#c2215564511191978655)

SSO between RDWeb and RDGateway is also not working internally. I have asked my RDS administrator to have a look into that. Will get back

[**Reply**](javascript:;)

1. 

[**Денис Яркин**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/16758498419546685955)[July 6, 2015 at 2:03 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1436209395176#c5925626378936085798)

Hello Tom!  
In your scenario, is RDWEB still uses FBA after ADFS authentication?

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17674111757513001655)[July 7, 2015 at 9:03 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1436321028085#c3200385208130635948)

Yes. You'll still need to login to RDWeb using the standard method, WAP in Server 2012 R2 does not support any kind of SSO pass through to RDWeb. That feature might be available in WAP 2.0 with Server 2016.

* 1. 

[**shubh**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/13006509687646399309)[July 8, 2015 at 6:32 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1436355155981#c9079525578411991208)

But strange thing which I have tested is, If we publish backend RDS as non claim aware application, SSO between WAP to RDWeb works but when we try to launch any application, it prompts for credentials once again and does not accept even if we use same credentials.

[**Reply**](javascript:;)

1. 

[**John F**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/04482240552539063037)[August 19, 2015 at 2:57 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1439971031281#c4561961632028572413)

Hi Tom,  
  
Thanks for the very helpful guide. I've published RDWeb using WAP with ADFS pre auth and integrated multi-factor auth. This works well however I now have the problem in that I can't use the "connect to a remote PC" function in RDWeb because of the pre-auth requirement I assume. My users have to connect to the RD Session Host and from there RDP to their PC. Do you know of a workaround to this problem?  
  
Also, has anyone been able to get SSO working on RDWeb to avoid the double sign in? I know you said it's not supported but hoping someone might have a solution.  
  
thanks.

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17674111757513001655)[August 19, 2015 at 6:49 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1440028192168#c3123083032592571013)

Hi John - check out the section above "Modifying Desktops.aspx" - that has instructions for modifying the "Connect to a remote PC" page to work with the pre-authentication.  
  
For your SSO question, Microsoft finally released their official guide for setting up RDG behind WAP - https://technet.microsoft.com/en-us/library/Dn765486.aspx - here is their explanation for SSO not working:  
  
"Authentication to the RD Web Access server will still use the RD Web Access form logon. This provides the least number of user authentication prompts as the RD Web Access logon form creates a client-side credential store that can then be used by Remote Desktop Connection client (mstsc.exe) for any subsequent Remote App launch."

* 1. 

[**John F**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/04482240552539063037)[August 20, 2015 at 12:24 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1440048282760#c5977217008153447671)

oops I completely missed that section. Thanks!

[**Reply**](javascript:;)

1. 

[**Денис Яркин**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/16758498419546685955)[August 19, 2015 at 3:43 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1439973836900#c4482962577908842008)

No, at now - SSO from RDWEB to RDP Session - not supported, actually ActiveX component get UserName and Password in plain text for authorisation on RDWEB logon page :) Waiting Windows 10, Server 10 and update in RDWeb :(

[Reply](javascript:;)

1. 

[**Jose Rivera**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17533257655495252698)[September 21, 2015 at 10:05 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1442891142592#c2541907109957396678)

Thank you for writing this article. It has cleared up alot of confusions! I have to say Citrix Netscaler seemed to have had all this figured out a long long time ago (in there own way of course).. but due to budget constraints this worked perfectly for our needs.

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17674111757513001655)[September 23, 2015 at 11:20 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1443025243223#c1176455318618974427)

Thanks, I'm glad others are finding this useful. :)

[**Reply**](javascript:;)

1. 

[**alekao@gmail.com**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/04264473090477214907)[February 25, 2016 at 9:39 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1456457953867#c818693746547628919)

Excellent article thank you! I am about to setup RDGateway in the DMZ using WAP and ADFS just as you have demonstrated. The only concern is that the existing WAP cluster servers are in a workgroup. I hope I can still publish the RDGateway using the ADFS relay party. If you have any new info on how to accomplish this, please share.

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17674111757513001655)[February 26, 2016 at 6:33 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1456533214448#c8584040158167297744)

I didn't try with the WAP servers in a workgroup. I know it did not work when the WAP servers were in a different untrusted domain though, so maybe you'll have better luck in a workgroup scenario.

* 1. 

[**Jukka Vähäaho**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/09896856155993419957)[March 1, 2016 at 3:45 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1456825504896#c264322045990361403)

Hi. Our WAP servers are also in DMZ. I have tried to get this work but RemoteApps do not start. Looks like ADFS authentication works and i can also logon to RD Web Access but when trying to start RemoteApp, Remote Desktop cannot connect to remotemachine. Reasons are your user account is not contained in RDG user list or remote machines computer name is in NetBIOS format. Is this expected behaviour when WAP-machines are not domain connected?

[**Reply**](javascript:;)

1. 

[**Unknown**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/10113218693585577047)[March 10, 2016 at 5:10 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1457608254597#c5582564085904997510)

Thanks for this beautifully written article.  
We've managed to get this working now but only through IE. I understand the point of this is to explicitly prevent using saved RDP files. Using other browsers like Chrome and Firefox downloads the RDP file which obviously doesn't run. Does this mean that we are limited to using only browsers that support ActiveX (i.e. Internet Explorer)? Or have I missed something?

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/01008287606632642530)[March 10, 2016 at 8:32 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1457620362361#c3792229653205494995)

You are correct in that only Internet Explorer will support this method. The RDP ActiveX control within IE handles passing the authentication cookie between the browser and mstsc.exe. Other browsers don't support ActiveX, and thus won't work. It'd be nice in the future if Microsoft would remove the requirement of ActiveX and instead find a way to replicate this functionality using HTML5 for cross-browser support.

[**Reply**](javascript:;)

1. 

[**Brian C. Campbell**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/16274969363329277767)[March 28, 2016 at 11:59 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1459184375633#c8384955266257599671)

Hi Tom,  
  
Thanks for the rare find regarding this info. It seems like ADFS 3.0 and WAP are not that often written about - I have come across more ADFS 2 and ADFS 4 preview articles than ADFS 3. I am struggling with making my way through ADFS and WAP with regard to publishing a simple internal hello world website. Are you aware of any other resources for publishing a non-claims-aware site? It seems the only examples I can find are sharepoint and OWA, but those are so Microsoft-richly-integrated that I dont know that the concepts are even the same for non-claims-aware relying party trust.  
  
Thanks,  
  
Brian

[Reply](javascript:;)

1. 

[**Unknown**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/01958919481988009446)[April 28, 2016 at 4:45 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1461879928532#c475700600969463028)

This posting was a great life saver. I really appreciate you taking the time to provide your documentation. I have a question regarding ADFS to RDWeb though. Is it possible to "Auto-fill" the username and/or password fields after authenticating from ADFS? I know that the end user is required to ALSO authenticate the RDWeb page, but is it possible to make it easier by auto populating the required fields?

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17674111757513001655)[April 30, 2016 at 10:01 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1462071701561#c6809805135753865439)

Not that I know of, but that would be convenient. Supposedly in Server 2016, there will be further integration between WAP and RDWeb that will allow single-sign on between the two.

[**Reply**](javascript:;)

1. 

[**Steffen Roch**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/14231134106488125185)[May 19, 2016 at 10:37 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1463672263997#c3542193016684977604)

Thanks Tom for that great post!  
  
In our scenario, RDWeb and RDGateway are hosted on different servers with different host names. How would the WAP and ADFS configuration need to be adjusted to cope with that setup?  
  
In the post you noted to "Enter the external URL that users will use to access your RD Gateway/RD Web Access installations" and to use the same name for the backend URL. That's working, when RD Gateway and RD Web Access are sitting on the same internal host. How to do this if they are on separate servers?

[Reply](javascript:;)

1. 

[**Peter**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17680916047061775891)[May 31, 2016 at 5:15 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1464732916585#c8480117113404268916)

Hi Tom,  
I was wondering about the Hotfix KB2982037. This site is not available anymore. Is it still required or is this fix included in never updates?

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17674111757513001655)[June 1, 2016 at 8:47 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1464832044718#c5841410467946117273)

Hi Peter. I'm not having issues getting to the KB article for 2982037. It appears Microsoft has included that hotfix with the 2975719 hotfix rollup - https://support.microsoft.com/en-us/kb/2975719

[**Reply**](javascript:;)

1. 

[**Peter**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17680916047061775891)[June 3, 2016 at 10:08 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1464966527327#c4779664557571880651)

Thank you very much Tom. I will continue my configuration. Your post is awesome.

[Reply](javascript:;)

[**Farrukh Khanzada**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/00638644723170112982)[August 23, 2016 at 8:08 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1472000926251#c3793697254928638074)

Thank you very much for this great post.  
Just adding that it works very well too if you select "Pass-through" under "Specify the preauthentication method" TAB. This way ADFS login page can be skipped and you can directly access RD Web login page.  
  
Only backdoor that I see is it allows direct connections to back-end resources when specifying GW settings in MSTSC but that can also be managed by limiting "RD Gateway-managed group members" in Resource Authorization Policies to RDSCB and RDSH servers for which access can be further controlled by applying server level restrictions.  
  
Cheers,

[Reply](javascript:;)

1. 

[**Mark**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/14481116735529518734)[September 1, 2016 at 2:37 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1472758676553#c367348205453259168)

I'm confused, should this work in Chrome/Firefox/etc? Because in those browsers it just downloads a .rdp file. And i'm not sure how opening that would "retrieve the ADFS edge token from the browser".

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Mark**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/14481116735529518734)[September 1, 2016 at 2:42 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1472758935306#c2721224510541482661)

Saw the other comment, disregard this.

[**Reply**](javascript:;)

1. 

[**Unknown**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17191323130280227560)[September 14, 2016 at 4:56 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1473890207125#c3675684823582421107)

I have followed this guide step by step but am still encountering an issue. I can pre-auth to rdweb then login to rdweb and launch an application but the application says failed login in every time and i cant get passed it. i dont think it is passing the cookie correctly to the gateway for auth. No matter what creds i enter they are never accepted. Any ideas?

[Reply](javascript:;)

1. 

[**Eric Hoy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17988262522599177901)[October 11, 2016 at 9:32 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1476196361173#c4592974501072227330)

Hi Tom,  
Great Article much appreciated, I have tried this a couple of times now and just cant get this working. Could I ask for some of your experience.  
  
Internally the RDS works fine.  
Externally the WAP server constantly attempts to service the RDS session.  
  
To explain further..  
- I browse to https://rdp.service.com  
- I get PreAuth'd by the ADFS portal  
- I login to RDWeb  
- Select my App, the popup is showing the SSL certificate is the 3rdParty SAN cert in my RDS server  
- I then get another RDP popup showing the selfsigned certificate of my WAP server.  
  
If you have any suggestions I would be very greatful, as I've been banging my head against this for a week!  
  
Many Thanks

[Reply](javascript:;)

1. 

[**Unknown**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/13943379673089905124)[January 17, 2017 at 2:55 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1484643305470#c4238214824473472110)

Hi Tom,  
  
Followed your guide, got everything working sweet... except: the clipboard redirection ONLY works when the client is able to 'Bypass RD Gateway for local address'.  
  
The only deviation from your guide is that my WAPs are in a DMZ AD forest and my ADFS and RD\* servers in an internal AD forest. There is a one way trust between the forests.  
  
You mentioned that you could only get things working properly when all the servers are in the same AD domain. Was one of the things that failed to work correctly the clipboard redirection?  
  
I can't for the life of me find any relevant info on the internet.  
  
Trautie

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17674111757513001655)[January 17, 2017 at 9:30 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1484710213780#c2472241877272576261)

My implementation had clipboard redirection explicitly disabled for security reasons, so I'm unable to comment.

[**Reply**](javascript:;)

[**maTTko**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/06690718912267270692)[February 2, 2017 at 4:00 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1486029605586#c969527908775616723)

Hello,  
  
I don't like the setup where you will authenticate ADFS, then WEB and then RDP GW. I create non-claim aware party trust, set KCD to SPN for the server hosting RDWEB and Gateway, reconfigure IIS from form authentication to windows integrated auth.  
  
Result:  
WAP -> adfs -> SSO to RDWEB: working great. THen you need to enter credentials when running rdp file.  
  
In my setup I am using everything HA. I reconfigure RDWEB to be running under service account (IIS app pool - instead of AppPoolIdentity, set permissions for the service account, policy for the account [logon as batch, ...]). Of course - update SPN to the service accoutn.  
  
problem:  
- internal NW: all working fine  
- external NW: error 401  
  
2nd try:  
update with service account as well RPC / RPC with cert  
- internal NW: all working fine  
- external NW: too many redirects  
  
on the WAP server are just some unclear errors in Event log.  
  
Did you or someone try to setup RDWEB / GW under service account behind WAP?

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17674111757513001655)[February 2, 2017 at 7:26 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1486085164278#c7818212619271694752)

No I don't believe I tried this configuration

* 1. 

[**Unknown**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/11216089279699480098)[May 11, 2017 at 6:58 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1494503910896#c9084928649074111657)

Hi, yes we have. Since we need high available rdweb we setup non-claims trust, and we also tried to make the rdweb application pool run as a user and put the SPN on the user. But havent got it working.. Seems no one has done it with nonclaims and loadbalancing rdweb...

* 1. 

[**Blackforce**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/02725766919265685967)[July 3, 2017 at 4:16 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1499073411829#c8832893359813355442)

Did anyone manage to get this working when the Gateway servers are load balanced? I have built a lab in Azure with an Azure internal Load balancer for the gateway. Seems hit and miss the logins

[**Reply**](javascript:;)

1. 

[**carreterock**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/01182303259670612082)[February 14, 2017 at 4:14 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1487110496599#c5996734758088659855)

Does anyone knows if there were any improvements in RDS 2016 and WAP?

[Reply](javascript:;)

1. 

[**mark fuller**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/02489945911603493065)[June 30, 2017 at 10:36 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1498837003255#c6239265184277839950)

Hi,  
  
Thanks for this guide it's brilliant. Question though I have users that use the rd client for iPad and iPhone and when I setup are rd remote app with adfs the client stops working. Do you know if the client supports this? Or is there extra config needed.  
  
Mark

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17674111757513001655)[July 5, 2017 at 2:16 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1499282202843#c3005511524033910156)

I do not believe this configuration will support iOS devices. WAP sends the token to RD Gateway via an ActiveX control, which isn't going to work w/ iOS.

[**Reply**](javascript:;)

1. 

[**Naudski**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/11699694777042265341)[August 15, 2017 at 2:21 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1502781669857#c7759228741283563369)

Hi,  
  
Is there anyone here who has overcome the credentials popup when launching a remote app or a remote desktop on the RDWeb page?  
I also have SSO to RDWeb through ADFS without the use of WAP.  
  
Arnaud

[Reply](javascript:;)

1. 

[**S Jaden**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/10434750061328639664)[November 25, 2017 at 9:24 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1511623473569#c3183125443757547865)

Intermediaries regularly have a fairly short lifetime, commonly 12 hours.[mexican vpn](https://web.archive.org/web/20180619155432/https:/www.how-to-hide-ip.net/browse-mexican-ip-address/)

[Reply](javascript:;)

1. 

[**Thomas**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/10518106786873838291)[February 20, 2018 at 3:34 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1519119277470#c3559769120230165143)

*This comment has been removed by the author.*

[Reply](javascript:;)

1. 

[**Thomas**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/10518106786873838291)[February 20, 2018 at 3:35 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1519119321760#c7021520151545990208)

Good day, is it possible to have the WAP server in another domain than the ADFS server? The environment has a seperate domain for all DMZ infrastructure. So WAP in DMZ domain and all other components in in internal domain. We are facing the problem that credentials are not passing correctly from ADFS to RDWeb page. In IE credentials are passed from ADFS to RDWeb, but you don't get to the actual app page. You reach the RDWeb page were credentials are filled, but you still need to click sign in. In Chrome no credentials are passed at all and you need to re-enter them. Hope I am clear enough... Anyone experience with this issue?

[Reply](javascript:;)

[Replies](javascript:;)

* 1. 

[**Tom Murphy**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17674111757513001655)[February 27, 2018 at 11:10 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1519751457697#c8879466435537374811)

Hi Thomas, theoretically it should be possible, and yes, having the WAP server in a perimeter network as either non-domain joined or joined to a perimeter domain network is certainly best practice, I was not able to get it working at the time.

[**Reply**](javascript:;)

1. 

[**Frank**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/17114830181976949834)[May 31, 2018 at 6:53 AM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1527767608355#c3931066488214216173)

*This comment has been removed by the author.*

[Reply](javascript:;)

1. 

[**Ariana**](https://web.archive.org/web/20180619155432/https:/www.blogger.com/profile/01767691539434563701)[June 5, 2018 at 12:05 PM](https://web.archive.org/web/20180619155432/http:/blog.tmurphy.org/2015/06/securing-rd-gateway-with-web.html?showComment=1528218344057#c534059876902167898)

This is due to the time a data packet travels back and forth from your VPN to the server. [https://novavpn.com/blog/popcorn-time/](https://web.archive.org/web/20180619155432/https:/novavpn.com/blog/popcorn-time/)

[Reply](javascript:;)

# ADFS: Deploy Active Directory Federation Services

[**Home**](https://www.petenetlive.com/)»[**General**](https://www.petenetlive.com/KB/Article/category/general)»ADFS: Deploy Active Directory Federation Services

**KB ID** 0001140

## Problem

The actual configuration of ADFS depends largely on what you intend to do with it. Here I’m using it to broker connections from my Microsoft Web Application Proxy. This article is just to ‘join the dots’ and covers just the installation of the role itself.

## Solution

**Before you Start**: Make sure you have a certificate ready to use for ADFS. I typically use a wildcard cert for this, it’s better if you have purchased one, or if you use certificate services, [here’s how to create a wildcard certificate](http://www.petenetlive.com/KB/Article/0001128).

**Note**: You can add adfs.{your-domain} to your wildcard as a SAN, (**Subject Alternative Name**), Also add certauth.adfs.{your-domain}. Yes, even on a wildcard certificate!

For example: ***adfs.petenetlive.com*** and ***certauth.adfs.petenetlive.com***.

You can either create a service account for ADFS to run under, or use a **GROUP MANAGED SERVICE ACCOUNT**.

### **What’s a Group Managed Service Account?**

It’s an AD object that acts as a service account, and you don’t need to worry about entering a password for it.

### **Create a Group Managed Service Account**

Before you can have a GSMA account you need a KDS Root Key in active Directory, to set that up, execute the following command;

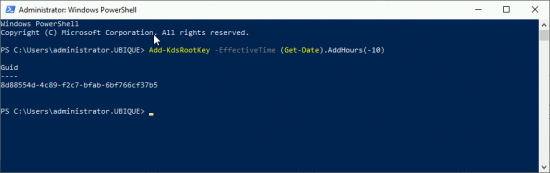
**If you have only one domain controller;**

Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10))

**If you have more than one domain controllers;**

Add-KdsRootKey –EffectiveImmediately

**If you use the second option you must then WAIT 10 HOURS!**

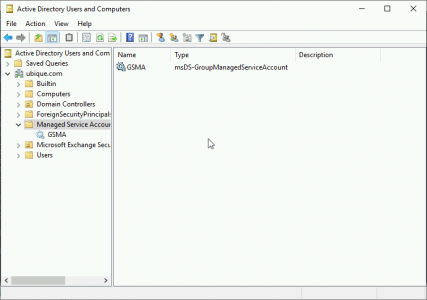
[](http://www.petenetlive.com/wp-content/uploads/2016/01/000.png)

Then go to a Domain Controller, and issue the following command;

New-ADServiceAccount -Name {Account-Name} -DNSHostname {DNS/DC-Name}

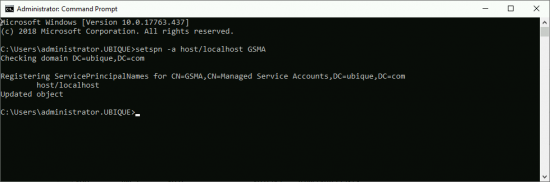
### **[Create Group Managed Service Account](http://www.petenetlive.com/wp-content/uploads/2016/01/000a.png)**

In case you are interested, you will then see it appear in Active Directory.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/000b.png)

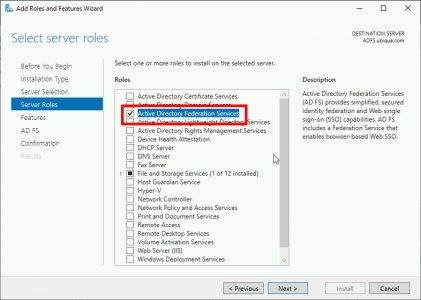
Then ON the ADFS Server, run the following command;

setspn -a host/localhost {GSMA-Account-Name}

[](http://www.petenetlive.com/wp-content/uploads/2016/01/000c.png)

### **Deploying Active Directory Federation Services**

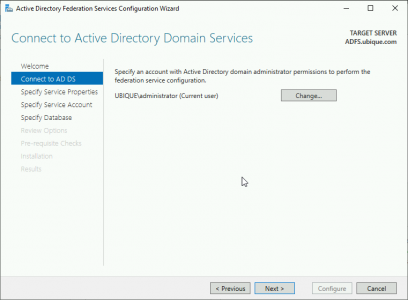
Server Manager > Manage > Add Roles and Features > Next > Next > Select the server > Next > Server Roles > Select Active Directory Federation Services > Accept all the defaults and install the role.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/004.png)

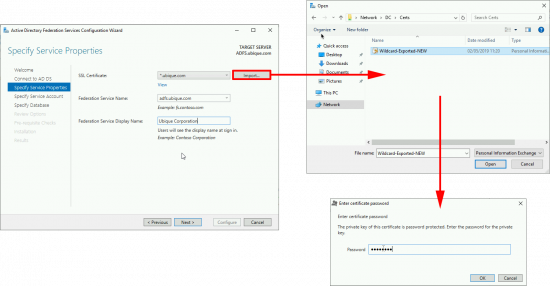
Launch the configuration wizard > Create the first federation server in a federation farm > Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/009.png)

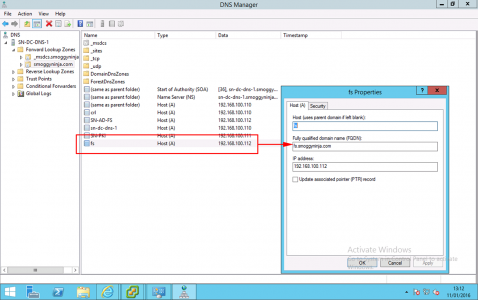
I’m setting this up while logged on as the domain administrator, so I’ll use that account to connect to AD > Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/010.png)

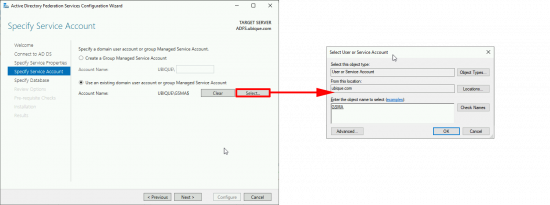
**WARNING**: If you use a wildcard cert like me it will choose the name of \*.{domain-name}. **THIS IS BAD!**Change the federation service name to something sensible, like adfs.domain.com. The ‘**Federation Service Display Name**‘ is what will be shown to the users as they authenticate. > Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/011.png)

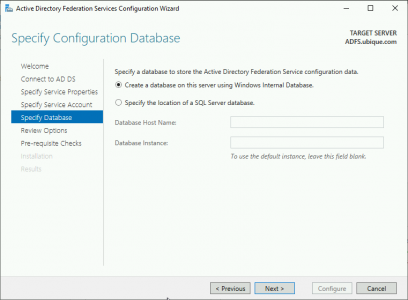
Make sure the federation server DNS name can be resolved in DNS! Remember if your Web Application Proxy server is in your DMZ, or outside the firewall, it will also need to be able to resolve this name, (I put them in the ‘***hosts***‘ file on my DMZ servers for this reason).

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00006-5.png)

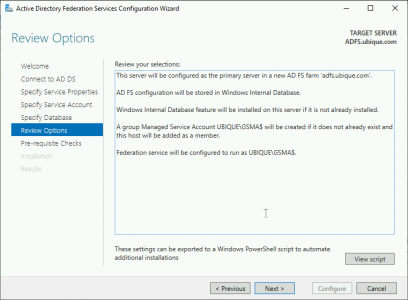
Enter your **Group Managed Service Account**, (created above) > Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/012.png)

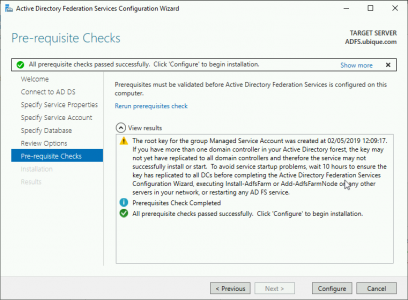
Create a database. (**Note**; If you are reinstalling it will discover any existing databases, and ask if you want to overwrite them) > Next.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/013.png)

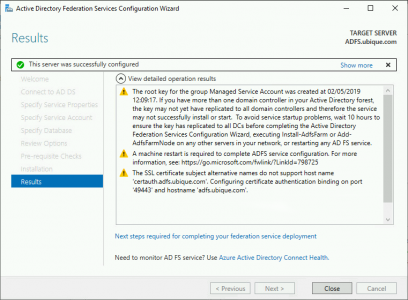
Next

[](http://www.petenetlive.com/wp-content/uploads/2016/01/014.png)

Configure.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/015.png)

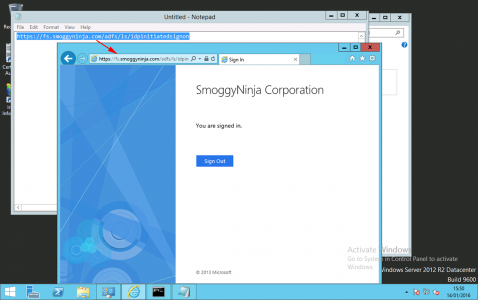
Close. (**Note**: I’ve got some warnings but all is well, trust me!)

[](http://www.petenetlive.com/wp-content/uploads/2016/01/016.png)

To test, open a web browser and go to ***https://{FQDN-Of FS-Service}/adfs/ls/idpinitiatedsignon*** and log in.

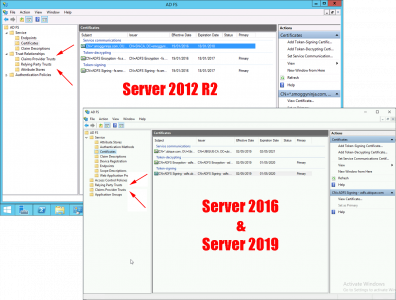
**Note**: If using Server 2016 or Server 2019, you have to enable this, or it will error! See the link below.

[**ADFS Test Page Error**](https://www.petenetlive.com/KB/Article/0001545)

[](http://www.petenetlive.com/wp-content/uploads/2016/01/00012-2.png)

At this point, how you proceed depends on what you are using Active Directory Federation Services for. You would set up either a relying or a claims provider trust next.

As said above I’m using this for Web Application Proxy. When that article is complete, I’ll put the link at the bottom of this article.

[](http://www.petenetlive.com/wp-content/uploads/2016/01/ADFS-Differnent-Trust-Folders.png)

## Related Articles, References, Credits, or External Links

[**Publishing Remote Desktop Services With Web Application Gateway**](http://www.petenetlive.com/KB/Article/0001143)